1. A transaction verification method wherein a user has a user account with identifying data unique to that user account, the method comprising:

communicating identifying data unique to a user account to a transaction terminal to authorize a transaction for that user account;

communicating a request for verification of the user account to a processing system, the processing system including access to stored authentication data and to identifying devices for a plurality of user accounts;

communicating a request for remote identification data to an identifying device associated with the user account for which verification is requested; and

communicating verification to the transaction terminal if remote identification data is communicated from the identifying device which sufficiently matches the stored authentication data associated with the user account for which verification is requested.

2. The transaction verification method of claim 1, further comprising denying the transaction at the transaction terminal if the remote identification data does not sufficiently match the stored authentication data.

3. The transaction verification method of claim 1, further comprising executing a default action stipulated by a profile if the remote identification data does not sufficiently match the stored authentication data.

4. The transaction verification method of claim 1, further comprising approving a transaction at the transaction terminal in response to the verification.

5. The transaction verification method of claim 1, further comprising communicating transactional information from the processing system to the user via the identifying device.

6. The transaction verification method of claim 5, further comprising enabling the user to disapprove the transaction in response to the transactional information.

7. The transaction verification method of claim 1, further comprising assigning a plurality of persons to the user account in addition to the user, wherein the plurality of users have at least some access to the user account.

8. The transaction verification method of claim 1, further comprising generating a profile.

9. The transaction verification method of claim 1, further comprising disapproving the transaction in response to determining a preprogrammed profile entry designating the transaction.

10. The transaction verification method of claim 1, further comprising initiating an action selected from a group of actions, each action associated with at least one profile, the group consisting of: selecting a type of the remote identification, selecting the identifying device, determining a characteristic pertaining to the transaction, an action based on the characteristic pertaining to the transaction, an action based upon an amount of money involved in the transaction, an action based upon a time of the

transaction, an action based upon a user preference, an action based upon a system preference and some other action based upon a programmatic rule.

11. The transaction verification method of claim 1, wherein the request for remote identification data does not reach the identifying device, communicating the request for remote identification to a second identifying device.

12. The transaction verification method of claim 1, wherein communicating the request for remote identification further includes communicating the request for remote identification data effectively simultaneously to a plurality of remote identification devices.

13. The transaction verification method of claim 1, wherein communicating the request for remote identification further includes prompting input used to select at least one of the identifying device and a type of the remote identification data.

14. The transaction verification method of claim 1, wherein communicating the request for remote identification further includes automatically determining at least one of the identifying device and a type of the remote identification data according to a particular of the transaction.

15. The transaction verification method of claim 1, wherein communicating the request for remote identification data to the identifying device includes communicating the request for remote identification data to an identifying device

selected from a group consisting of at least one of: a cellular telephone, a pager, a personal digital assistant, a global positioning receiver and a hand held device.

16. The transaction verification method of claim 1, wherein communicating the remote identification data includes communicating remote identification data from a delegate authorized to act on behalf of the user.

17. The transaction verification method of claim 1, further comprising retrieving the stored authentication data from a memory remote from the processing system.

18. The transaction verification method of claim 1, wherein receiving the remote identification data includes receiving live capture data.

19. The transaction verification method of claim 1, wherein receiving the remote identification data includes retrieving stored data from memory.

20. The transaction verification method of claim 1, further comprising communicating the remote identification data from the identifying device to the processing system.

21. The transaction verification method of claim 1, wherein communicating the identifying data further includes authorizing the transaction if the identifying data is communicated within a predetermined transaction time period.

22. The transaction verification method of claim 1, wherein communicating the identifying data further includes denying the transaction if the identifying data is communicated outside of a predetermined transaction time period.

23. The transaction verification method of claim 22, wherein communicating the identifying data further includes authorizing the transaction if the identifying data is communicated within a subsequent period outside of the predetermined transaction time period.

24. The transaction verification method of claim 1, further comprising, on a subsequent attempt by the user to authenticate, causing the user to provide the remote identification data to the identifying device without providing an ID.

25. The transaction verification method of claim 1, wherein communicating the verification further includes communicating remote identification data selected from a group comprising: a token, a password, a biometric record and proximity data descriptive of a location of the identifying device.

26. The transaction verification method of claim 1, wherein communicating the verification further includes communicating the verification only if remote identification data is communicated from multiple users.

27. The transaction verification method of claim 1, wherein communicating the verification further includes communicating the verification only if remote identification data is communicated from a percentage of multiple users.

28. The transaction verification method of claim 1, further comprising disapproving a transaction at the transaction terminal in response to the verification.

29. The transaction verification method of claim 1, further comprising temporarily disabling the transaction verification method.

30. The transaction verification method of claim 1, further comprising storing the stored authentication data in association with a second account.

31. The transaction verification method of claim 1, further comprising storing the remote identification data as updated stored authentication data in response to a sufficient match.

32. A transaction verification method wherein a user has a user account with identifying data unique to that user account, the method comprising:

communicating identifying data unique to a user account to a transaction terminal to authorize a transaction for that user account;

communicating a request for verification of the user account to a processing system, the processing system including access to stored authentication data and to identifying devices for a plurality of user accounts;

communicating a request for remote identification data to an identifying device associated with the user account for which verification is requested;

communicating remote identification data from the identifying device in response to the request therefore; and

determining if the remote identification data communicated from the identifying device sufficiently matches the stored authentication data associated with the user account for which verification is requested, and if it does, communicating verification to the transaction terminal.

33. A transaction verification method wherein a user has a user account with identifying data unique to that user account, the method comprising:

communicating identifying data unique to a user account to a transaction terminal to authorize a transaction for that user account;

communicating a request for verification of the user account to a processing system, the processing system including access to stored authentication data and identifying devices for a plurality of user accounts;

communicating a request for remote identification data to an identifying device associated with the user account for which verification is requested;

communicating remote identification data from the identifying device in response to the request therefore; and

determining if the remote identification data communicated from the identifying device sufficiently matches the stored authentication data associated with the user account for which verification is requested.

34. The transaction verification method of claim 33, further comprising communicating verification to the transaction terminal if it is determined that the remote identification data sufficiently matches the stored authentication data.

35. A transaction verification method wherein a user has a user account with identifying data unique to that user account, the method comprising:

communicating identifying data unique to a user account to a transaction terminal to authorize a transaction for that user account;

communicating a request for verification of the user account to a processing system, the processing system including access to identifying devices for a plurality of user accounts;

communicating a request for remote identification data to an identifying device associated with the user account for which verification is requested, wherein the identifying device has access to stored authentication data; and

communicating verification to the transaction terminal if remote identification data is communicated to the identifying device sufficiently matches the stored authentication data associated with the user account for which verification is requested.

36. A transaction verification method wherein a user has a user account with identifying data unique to that user account, the method comprising:

communicating identifying data unique to a first user account to a transaction terminal to authorize a transaction for the first user account;

communicating a request for verification of the first user to a processing system, the processing system including access to stored authentication data and identifying devices for a plurality of user accounts;

communicating a request for remote identification data to an identifying device associated with a second user; and

communicating verification to the transaction terminal if remote identification data is communicated from the identifying device which sufficiently matches the stored authentication data associated with the second user.

37. The method of claim 36, further comprising approving the transaction in response to the sufficient match and affirming input from the second user.

38. The method of claim 36, further comprising denying the transaction in response to input from the second user.

39. A transaction verification method wherein a user has a user account with identifying data unique to that user account, the method comprising:

communicating remote identification data and a transaction terminal identification from an identifying device associated with a user account to a processing system, the processing system including access to stored authentication data and to identifying devices for a plurality of user accounts; and

in response to a request for verification from a transaction terminal, communicating verification to the transaction terminal if the transaction terminal is identified by the transaction terminal identification and the remote identification data communicated from the identifying device sufficiently matches stored authentication data associated with the user account.

40. An apparatus, comprising:

a transaction terminal for authorizing a transaction configured to receive identifying data unique to a user account;

an identifying device associated with the user account and configured to receive remote identification data from a user in response to a request for remote identification data;

a processing system in communication with the identifying device including access to stored authentication data and identifying devices for a plurality of user accounts, wherein the processing system receives the remote identification data from the identifying device; and

program code executed by the processing system configured to both initiate sending the request for remote identification data to the identifying device and to send verification to the transaction terminal after determining if the remote identification data matches the stored authentication data.

41. The apparatus of claim 40, wherein the program code initiates denying the transaction at the transaction terminal if the remote identification data does not sufficiently match the stored authentication data.

42. The apparatus of claim 40, wherein the program code initiates executing a default action included in a profile if the remote identification data does not sufficiently match the stored authentication data.

43. The apparatus of claim 40, wherein the program code initiates approving the transaction at the transaction terminal in response to the verification.

44. The apparatus of claim 40, wherein the program code initiates communicating transactional information from the processing system to the user via the identifying device.

45. The apparatus of claim 40, wherein the user disapproves the transaction in response to the transactional information.

46. The apparatus of claim 40, wherein the user comprises a plurality of persons including access to the user account.

47. The apparatus of claim 40, wherein the program code initiates generating a profile.

48. The apparatus of claim 40, wherein the program code initiates disapproving the transaction in response to determining a preprogrammed profile entry designating the transaction.

49. The apparatus of claim 40, wherein the program code initiates communicating the request for remote identification to a second identifying device when the request for remote identification data does not reach the identifying device.

50. The apparatus of claim 40, wherein the program code initiates determining the identifying device from a profile.

51. The apparatus of claim 40, wherein the identifying device is selected from a group consisting of at least one of: a cellular telephone, a pager, a personal digital assistant, a global positioning receiver and a hand held device.

52. The apparatus of claim 40, wherein the remote identification data is selected from a group consisting of at least one of a: password, user identifier, token, geographic position and biometric record.

53. The apparatus of claim 40, wherein the stored authentication data is retrieved remotely from the processing system.

54. The apparatus of claim 40, wherein the remote identification data comprises live capture data.

55. The apparatus of claim 40, wherein the remote identification data is retrieved from memory.

56. The apparatus of claim 40, wherein the program code, on a subsequent attempt by the user to authenticate, causes the user to provide the remote identification data to the identifying device without providing an ID.

57. The apparatus of claim 40, wherein the remote identification data includes proximity data descriptive of a location of the identifying device.

58. The apparatus of claim 40, wherein the transaction terminal disapproves the transaction in response to the verification.

59. The apparatus of claim 40, wherein the program code initiates temporarily disabling verification processes.

60. The apparatus of claim 40, wherein the program code initiates storing the stored authentication data in association with a second account.

61. The apparatus of claim 40, wherein the program code initiates storing the remote identification data as updated stored authentication data in response to a match.

62. The apparatus of claim 40, wherein the remote identification data is provided by a different user than a user who initiated the transaction.

63. The apparatus of claim 62, wherein the transaction is approved only in response to the sufficient match and affirming input from the different user.

64. The apparatus of claim 62, wherein the transaction is denied in response to disaffirming input from the different user.

65. An apparatus, comprising:

a transaction terminal for authorizing a transaction configured to receive identifying data unique to a user account;

an identifying device associated with the user account and configured to receive remote identification data from a user in response to a request for remote identification data, the identifying device including access to stored authentication data;

program code executed by the identifying device configured compare the remote identification data to the stored authentication data to determine if there is a sufficient match, and to generate a signal communicating the results of the comparison; and

a processing system including access to the identifying device, along with a plurality of other identifying devices, wherein the processing system communicates verification to the transaction signal in response to receiving the signal from the identifying device.

66. A program product, comprising:

a program resident on a processing system including access to stored authentication data, and identifying devices for a plurality of user accounts, as well as to remote identification data from an identification device associate with a user account, wherein the program determines if the remote identification data matches the stored authentication data and initiates communicating verification to a transaction terminal configure to authorize a transaction in response to the verification; and

a signal bearing medium bearing the program.

67. The program product of claim 66, wherein the signal bearing medium includes at least one of a recordable medium and a transmission-type medium.